CHAPTER 8

SECURITY

A security clearance is a determination, made from all available information, that an individual is eligible for access to classified information to a specified level or, in some cases, is eligible for assignment to other positions of trust. The clearance tells you someone is eligible for access; it does not give that person access authorization. It is important to separate these two processes: granting clearance and granting access. An individual may remain **eligible** for access even though the person's present position does not require access to classified information.

No person will be given access to classified information unless a favorable determination has been made of the person's loyalty, reliability, and trustworthiness. The initial determination is based on a personnel security investigation (PSI). Only commanders, commanding officers (COs), chiefs of recruiting stations, and the Director of Central Adjudication Facility are authorized to request PSIs on personnel under their jurisdiction.

The Defense Security Service (DSS) or, where specified, the Office of Personnel Management (OPM) conducts or controls all PSIs for the Department of the Navy. Requests for PSIs must be kept to the absolute minimum. They will not be submitted on any civilian or military personnel who will retire, resign, or separate with less than 9 months of service remaining.

TYPES OF PERSONNEL SECURITY INVESTIGATIONS

A PSI is an inquiry into an individual's activities; it is used for the specific purpose of making a personnel security determination. Investigations such as those conducted for current criminal activity, espionage, compromise, or subversion have an impact on employment, clearance, or assignment, but are not classified as PSIs.

There are a total of eight PSI categories listed in the *Department of the Navy (DON) Personnel Security Program (PSP) Regulation*, SECNAVINST 5510.30 series. As a YN, you will probably only work three of these: the National Agency Check (NAC), Single-Scope Background Investigation (SSBI), and Periodic Reinvestigation (PR).

NATIONAL AGENCY CHECK

An NAC is a search of the files of federal agencies for information about the person being investigated. The DSS conducts the check. An NAC includes, as a minimum, a check of the Defense Clearance and Investigations Index (DCII) and the FBI files. If either of those checks reveals information that warrants further study, the DSS checks the files of other agencies.

A person who wishes to enter military service undergoes an entrance NAC (ENTNAC). The ENTNAC determines the suitability of an individual for entry into the service.

The PSI request package for an NAC will be submitted to DSS using the SF 85P, Questionnaire for Public Trust Positions, and an FD 258, Applicant Fingerprint Card.

SINGLE-SCOPE BACKGROUND INVESTIGATION

The SSBI, conducted by the DSS, provides a greater depth of knowledge than an NAC. Elements covered in an SSBI include the subject's education, neighbors, foreign travel, foreign connections, and organizational affiliations. DSS does not conduct a subject interview as part of an SSBI, except to resolve unfavorable or questionable information. An SSBI also includes an NAC of the subject's spouse or cohabitant and any other members of the subject's immediate family 18 years of age or older who are U.S. citizens other than by birth or who are not U.S. citizens. The scope of an SSBI is 10 years before the investigation or from the 18th birthday to the time of the investigation, whichever is the shorter period; however, at least the last 2 years must be covered. No investigation may extend further back than the subject's 16th birthday. SSBIs are conducted only when specifically required by CNO or higher authority.

The SSBI request will be submitted to DSS using a DD1879, DoD Request for Personnel Security Investigation (original and two copies); SF 86, Questionnaire for National Security Positions (original and four copies); and FD 258, Applicant Fingerprint Card (original and one copy).

PERIODIC REINVESTIGATION

A PR determines a subject's continued eligibility for access to classified information by reevaluating a previous valid investigation of the person. PRs are conducted every 5 years and should be initiated 4 years 6 months from the completion date of the last investigation. PR elements include an NAC; a subject interview; credit, employment, and local agency checks; interviews of employers; and character references, to include former spouses.

INVESTIGATIVE REQUIREMENTS FOR A PERSONNEL SECURITY CLEARANCE

The investigative requirements for a personnel security clearance apply to positions involved with access to classified information. The requirements are based on the PSI prescribed for the specific classification level—Top Secret, Secret, or Confidential—to be accessed in one's everyday duties.

TOP SECRET

The investigative basis for a Top Secret clearance is the completion of a favorable SSBI or PR. For those who have continuous assignment or access to Top Secret, critical sensitive positions, sensitive compartmented information (SCI), Nuclear Weapon Personnel Reliability Program (PRP) positions, and other such programs (as outlined in chapter 6 of the *PSP*), the SSBI must be updated every 5 years by a PR. This PR must be submitted within 30 days following granting of the clearance.

SECRET/CONFIDENTIAL

The investigative basis for a Secret or Confidential clearance is a favorable ENTNAC for first-term military enlistees. The ENTNAC remains valid throughout the person's enlistment, provided no break in service greater than 12 months occurs. Secret and Confidential clearances must be updated every 10 and 15 years, respectively. Members assigned to PRP and some other sensitive programs must have their clearances updated every 5 years by a PR.

NOTE: The *Nuclear Weapon Personnel Reliability Program (PRP)*, SECNAVINST 5510.35 series, a program that you, as a YN, may frequently encounter, provides the standards of individual reliability required for personnel performing duties involving nuclear weapons and components. PRP requires commands to screen personnel before transferring them to training leading to PRP assignment. The investigative requirements for PRP assignment are based on the position designation. PRP positions are designated as either **critical** or **controlled**.

Critical: The minimum investigative requirement for initial assignment is a valid SSBI completed within the past 5 years. This requirement may be satisfied by a valid favorable PR. If there is no investigation to satisfy the requirement for initial assignment, the command must request an SSBI. A PR is required every 5 years.

Controlled: The minimum investigative requirement for initial assignment is a valid favorable SSBI completed within the past 5 years. This requirement may be satisfied by a valid favorable ENTNAC, NAC, SSBI, or PR completed within the past 5 years. When no investigation has been conducted to satisfy the requirements for initial assignment, the command must request a new NAC.

When an individual is transferred from one PRP assignment to another, the record of prior investigation will be accepted in rescreening the individual at the new assignment.

DEPARTMENT OF THE NAVY CENTRAL ADJUDICATION FACILITY

The Department of the Navy Central Adjudication Facility (DON CAF) was established to provide central evaluation of individuals receiving security clearances. This facility is the sole authority to grant, deny, or revoke security clearances for all Department of the Navy (DON) personnel. The DSS and the Office of Personnel Management (OPM) forward all completed PSIs to DON CAF. The facility then determines eligibility for security clearances or assignment to sensitive duties. Upon making a favorable security clearance/eligibility determination, DON CAF will notify the command by message, letter,

or Manpower Management System (MMS), as appropriate.

REQUESTS FOR DON MILITARY PERSONNEL

All requests for extensions of interim clearances, security clearance revalidations, notification of administrative downgrading or withdrawal of clearances, and reports of derogatory information are submitted to DON CAF via the Personnel Security Action Request.

REVALIDATION UPON TRANSFER/ ACCESS TO SPECIAL ACCESS PROGRAMS

When an individual who has a security clearance transfers to a new command into a duty assignment requiring access to special access program information, the gaining command revalidates the security clearance and submits a Personnel Security Action Request for clearance at the level needed by the person to perform those duties.

INTERIM CLEARANCES

Interim clearances may be granted temporarily (for 180 days), pending completion of full investigative requirements or revalidation of security clearances from DON CAF. An extension may be granted beyond the 180 days provided the agency notifies DON CAF 30 days before the expiration of an interim clearance. COs should send DON CAF a tracer action using the Personnel Security Action Request. A copy of these documents must be maintained in the individual's service record or security file until the investigation and final clearance determination are completed.

PERSONNEL SECURITY ACTION REQUEST

The Personnel Security Action Request, as stated previously, is used to request security determinations from DON CAF. Complete instructions for completing this request are on the back of the form. When the command receives the answer from DON CAF, it is attached to the member's Record of Investigation, Clearance, and Access, OPNAV 5520/20, and retained in the member's service record. Copies of all correspondence relating to clearances may be obtained for command security files.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT, SF312

The primary purpose of the Classified Information Nondisclosure Agreement, SF312, is to inform individuals of the trust placed in them by their authorized access to classified information. The agreement also informs them of their responsibilities to protect that information from unauthorized disclosure and of the consequences that may result from their failure to meet those responsibilities.

All persons with authorized access to classified information are required to sign this form. The most opportune time for a person to sign this form is during preparation of the paperwork requesting clearance authorization from DON CAF. Although the information contained in this form is quite lengthy, the individual should read the form in its entirety before signing it.

The execution of the form must be personally witnessed by the individual's CO, executive officer, security manager, or supervisor. The witnessing official must sign and date the agreement at the time it is executed. An OPNAV 5520/20 entry will be made to indicate that the individual has executed an SF312. Should the individual lose access to classified information for any reason, the form will also be used for security debriefing.

INFORMATION SECURITY

For the protection of the interests of the United States, certain information is unavailable to other countries. This information is given a classification that determines how much protection it needs. The level of classification is based on how much damage would be caused if other countries could obtain it. This section provides you with the categories of classification, the rules regarding the safeguarding of each level, and your responsibilities in handling classified material.

CLASSIFIED MATERIAL

As discussed in chapter 2, the *Department of the Navy (DON) Information Security Program (ISP) Regulation,* SECNAVINST 5510.36 series, provides the basis of the Navy's program for safeguarding classified information. It was written based on requirements made at the national level and provides the procedures and requirements we use on a daily basis. From the Secretary of the Navy, to the Chief of

Naval Operations, to your CO, to your command security manager, to you, this instruction lays down specific responsibilities and procedures to protect classified information. Every individual who acquires access to classified material is responsible for protecting it. As a YN, you will be directly involved in this process and must be aware of the regulations given in this element of the security manuals.

The purpose of the security program is to ensure that official information is protected to the level and for the period of time necessary. Essential policies and procedures have been established to monitor the Navy's security program. The effectiveness of this monitoring is ensured through the process of identifying the information to be protected, defining a progressive system for classification, downgrading the level of classification, and, finally, declassifying the information when appropriate.

The security of the United States, in general, and of naval operations, in particular, depends upon the success of the security program. Don't let information fall into the wrong hands through careless talk or improper handling and safeguarding of written information.

CATEGORIES OF CLASSIFIED INFORMATION

Information is classified into three categories, each category requiring its own level of protection: Top Secret, Secret, and Confidential.

Top Secret

Top Secret is the designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause **exceptionally grave damage** to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communication intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

Secret

Secret is the designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause **serious damage** to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

Confidential

Confidential is the designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause **identifiable damage** to the national security. Examples of identifiable damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test data, design, and production data on munitions of war.

NOTE: You will come across information marked **For Official Use Only**. This is not a category of classification under the information security program.

You should refer to the *PSP* for the requirements of each type of investigation and the level of clearance authorized by each.

CONTROL OF DISSEMINATION

The CO is responsible for controlling the dissemination of classified material within the command. The command security manager is delegated the responsibility to ensure information is issued and personnel are instructed on prevention of unauthorized disclosure of classified information. Steps must be taken to ensure that the existence, contents, and whereabouts of classified information are divulged only to those who are authorized access and whose official duties require that knowledge.

Responsibility for determining who sees classified information rests upon each individual who has possession or knowledge of the information, not the person who seeks the information. You must be totally satisfied that you are providing information to a properly authorized person.

ACCOUNTABILITY AND CONTROL

Regulations do not guarantee protection—enforcing them does. The following procedures are required by the security regulations, and one of your responsibilities is to know and enforce these accountability and control procedures. Remember, the security program is a means, not an end.

Top Secret Accountability

Each copy of a Top Secret document is numbered at origination with the copy number and total number of copies created. For example:

Copy number 2 of 10 copies

Each copy of the document will include a list of effective pages with a record for page checks. Further, each page of Top Secret letters or messages is numbered as shown below.

Page 1 of 15 pages

Top Secret documents cannot be reproduced without permission of the issuing or higher authority. When permission is granted, any copies made must also be numbered. Always use the number of the original the copies are made from as a part of the numbering sequence. For example:

Copy 14/1 of 2 copies

The 14 indicates the fourteenth copy of the original.

Top Secret material is always transported hand to hand and receipted for at each exchange.

The security manager or the Top Secret control officer makes inventory for all Top Secret material at least annually and at each change of command.

Top Secret Control

A Disclosure Record, OPNAV Form 5511/13, identifying the document and all personnel who have had access to the document, is maintained for each individual document. The record of disclosure is maintained for 2 years after the document is transferred, downgraded to a lower classification, or destroyed.

Secret Accountability

A command must establish administrative procedures to record Secret material originated or held by the command. The record can be in the form of a log, a route slip file (Correspondence/Material Control Form 5216/10), a serial file, or some other administrative record.

Secret Control

The control procedures for Secret material must balance security and operating efficiency. The normal procedure is hand-to-hand transfer between individuals, but receipt at each transfer within a command is not required.

Confidential Accountability and Control

Procedures for protecting Confidential material are less stringent than those for Secret material. There is no requirement to maintain records of receipts, distribution, or disposition of Confidential material. Measures are required, however, to protect it from unauthorized disclosure by controlling access and ensuring proper marking, storage, transmission, and destruction.

Serial Numbers

The *Department of the Navy Correspondence Manual*, SECNAVINST 5216.5 series, prescribes that classified correspondence be serially numbered by the originator for each calendar year. A serial number is one of a consecutive group of Arabic numerals assigned to a specific piece of correspondence for identification purposes. A separate consecutive group of numbers is used for each security classification, and this group of numbers is totally separate and distinct from the unclassified correspondence serial file numbers. Serial numbers of Confidential letters are preceded by the letter **C**; those for Secret, by **S**; and for Top Secret, by **TS**.

CUSTODIAL PRECAUTIONS

Classified material is not removed from the physical confines of a command without the knowledge and approval of the CO or an authorized representative. When classified material is removed, a complete list is prepared, signed by the individual removing the material, and appropriately filed until the material is returned.

Care During Working Hours

Each person in the Navy must take every precaution to prevent deliberate or casual access to classified information by unauthorized persons. The following are precautions that must be followed:

- When classified documents are removed from stowage for working purposes, the documents are to be kept under constant surveillance or face down or covered when not in use. At no time will classified material be left unattended.
- Any items used to prepare classified material must be destroyed or safeguarded according to the classification of the material they are used to produce. These items include drafts, carbon sheets, carbon paper, correctable film typewriter ribbons, fabric typewriter ribbons only used once, plates, stencils, stenographic notes, worksheets, and similar items. After the upper and lower sections of a fabric typewriter ribbon have been cycled through the typewriter at least five times, the ribbon may be treated as unclassified.
- Classified material, upon receipt, is opened by the addressee or by persons specifically authorized by the addressee in writing to open material of the grade or classification involved.
- If, for any reason, a room must be vacated during working hours, any classified material therein must be stowed according to stowage instructions for the classification involved.

Care After Working Hours

A system of security checks at the close of each working day must be instituted to make sure that classified material held by a command is properly protected. Custodians of classified material must make an inspection to ensure the following requirements have been met:

- Burn bags are properly stowed or destroyed.
- The contents of wastebaskets that contain classified material are properly stowed or destroyed.
- Classified shorthand notes, carbon paper, typewriter ribbons, rough drafts, and similar papers are properly stowed or destroyed. As a matter of routine during the day, such items must be placed in burn bags as soon as they have served their purpose.

Identification of the individual responsible for the contents of each container of classified material must be readily available. The individual so identified is contacted in the event a container of classified material is found open and unattended.

Care of Working Spaces

The necessary safeguards must be afforded to buildings and areas in which classified information is kept. Precautions must also be taken to minimize any danger or inadvertent disclosure of classified material in conversations. You must not discuss classified information in public places.

Care During Emergencies

Commands are responsible for establishing detailed procedures and responsibilities for the protection of classified material in the case of natural disasters, civil disturbances, or enemy action. Your command's emergency bill should provide for guarding, removing, or destroying classified material on a priority basis.

TRANSMISSION OF CLASSIFIED MATERIAL

The term **transmission** refers to any movement of classified material from one place to another. The basic rule is that the material must be in the custody of an appropriately cleared individual or in an approved carrier system.

Transmission requirements are basic in nature. Refer to the *ISP* for complete details.

Top Secret

Top Secret material cannot be mailed. It must be hand-carried by the Armed Forces Courier System (ARFCOS), the Department of State Courier System, specifically cleared and designated personnel, or transmitted by way of a fully protected cryptographic system.

Secret

Secret material may be transmitted in the same manner as Top Secret or mailed in the U.S. Postal Service registered mail system.

Confidential

Confidential material may be transmitted by any means suitable for Secret material. First-Class Mail service may be used between DoD activities in the United States or its territories. Material going to overseas APO or FPO addresses is sent by registered mail.

RECEIPT SYSTEM

Top Secret material is covered by a continuous chain of receipts. Secret material, at a minimum, is covered by a receipt between commands and other authorized addressees. Receipts for Confidential material are not required. The receipt form is attached to or enclosed in the inner cover.

Postcard receipt forms are unclassified and are used whenever practical. The form contains only such information as is necessary to identify the material being transmitted. Receipts are retained for a minimum of 2 years.

When a flyleaf (page check) form is used with classified publications, the postcard receipt is not required.

The Record of Receipt, OPNAV Form 5511/10, should be used in receipting for classified material.

PREPARATION FOR TRANSMISSION AND SHIPMENT

Whenever classified material is transmitted, it should be enclosed in two opaque, sealed envelopes or similar wrappings, where size permits, except as follows:

- Classified written material should be folded or packed so that the text will not be in direct contact with the inner envelope or container.
- The inner envelope or container shows the address of the receiving activity; the highest classification of the material enclosed including, where appropriate, the Restricted Data marking; and any special instructions. It should be carefully sealed to minimize the possibility of access without leaving evidence of tampering. Attach the receipt form (if required).
- The outer cover should not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified. The outer cover of Confidential material being transmitted by United States Postal Service First-Class Mail should be marked **FIRST CLASS** and be endorsed **POSTMASTER: DO NOT FORWARD, RETURN TO SENDER**.

Whenever the classified material being transmitted is too large to prepare as described above, it should be enclosed in two opaque, sealed containers, such as boxes or heavy wrappings, or prepared as follows:

- If the classified material is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure.
- If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable (such as a missile), the outside or body of the item may be considered as the outer enclosure, provided the shell or body is not classified.
- If the classified material is an item of equipment that is not reasonably packageable and the shell or body is classified, it should be draped with an opaque covering that will conceal all classified features. The coverings must be capable of being secured so as to prevent inadvertent exposure of the item.
- Specialized shipping containers, including closed cargo transporters, may be used instead of the above packaging requirements. In such cases, the container may be considered to be the outer wrapping or cover.
- Material used for packaging should be of such strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to help detect any tampering with the container.

The wrappings should conceal all classified characteristics. Activities will provide for the stocking of several sizes of cardboard containers and corrugated paper. Packages must be sealed with tape that will retain the impression of any postal stamp, preferably brown paper tape. Bulky packages must be inspected to determine whether the material is suitable for mailing or whether you should transmit it by other approved means.

Closed and locked compartments, vehicles, or cars should be used for shipments of classified material except when another method is authorized by the

consignor. In any event, individual packages weighing less than 200 pounds gross should be shipped in a closed vehicle.

ADDRESSEES

Classified material is normally addressed to a recognized activity and not to an individual. Office code numbers; office or division titles, such as Training Division; or similar aids in expediting internal routing may be used in addition to the organization address.

For correct mailing addresses, consult the current issue of the *Standard Navy Distribution List,* which contains the official list of fleet and mobile units, their administrative addresses, and the official list of shore activities with complete administrative addresses.

The inner envelope or container must show the address of the receiving activity.

An outer envelope or container must show the complete and correct address and the return address of the sender. However, the address may be omitted from the outer enclosure for shipment in full truckload or carload lots.

Care must be taken to make sure that classified material intended only for the United States elements of international staffs or other organizations is addressed specifically to those elements.

STOWAGE

Classified material is stowed only at locations where suitable facilities are available. The *ISP* details the requirements for storing material at each level of classification.

Do not store valuables such as money, jewelry, or precious metals in the same containers as classified material. They increase the risk of a container being illegally opened or stolen.

For emergency purposes, the identity of persons having access to the container and a symbol indicating the relative priority of destruction are posted on the container. In no case, however, should the level of classified material inside the container be shown.

DESTRUCTION OF CLASSIFIED MATERIAL

Classified material must be destroyed by burning, melting, shredding, or other forms of mutilation that prevent reconstruction of the material.

RECORDS OF DESTRUCTION

Top Secret and Secret material destruction must be recorded. Use Classified Material Destruction, OPNAV Form 5511/12, or any other type of record, as long as it includes space for complete identification of the material, number of copies destroyed, and date of destruction.

Both Top Secret and Secret material require two officials to witness the destruction and sign the destruction report. Officials responsible for destruction must have a clearance equal to or greater than the material being destroyed. The record of destruction is kept on file for 2 years.

When either Top Secret or Secret material is placed in a burn bag for central destruction, the witnessing official(s) should sign the destruction record at the time the material is actually placed in the bag. Burn bags are afforded the same protection as the highest level of material they contain and must be handled by appropriately cleared personnel.

SECURITY VIOLATIONS

Whether intentional or not, and whether material is compromised or not, the fact that a procedure was not followed or was incorrectly performed and could have caused damage places the person responsible for the compromise in line for disciplinary action. Safeguarding classified material is a daily priority.

If a container is found open or unlocked, report it immediately to someone in authority. A check must be made as soon as possible to see if compromise was possible.

If you receive classified material that was transmitted incorrectly, notify the CO of the sending unit with a Security Discrepancy Notice, OPNAV Form 5511/24.

Finally, bring an improperly marked classified document to the attention of the originator, also with the Security Discrepancy Notice, OPNAV Form 5511/24.

SUMMARY

This chapter has introduced you to the basic methods used to process personnel security clearances and to classified material control. This area is of extreme importance to the safeguarding of classified material and, consequently, to the safety of your unit

and to the country. The best means of protecting our country's interests is to ensure only qualified personnel are given access through a valid investigative process.

This chapter provides basic information only. The *Department of the Navy (DON) Information Security Program (ISP) Regulation,* SECNAVINST 5510.36 series, and *Department of the Navy (DON) Personnel Security Program (PSP) Regulation,* SECNAVINST 5510.30 series, provide detailed information, such as specific preparation requirements for reports and visit requests. YNs, no matter what their rank, should become proficient with the contents and use of these two extremely important instructions.